CLAIMS – MARK-UP COPY

1. (Currently Amended) A computer-implemented method for securely transmitting an information package from a sender to an addressee via a network, the method comprising the steps of:

~~determining~~ searching at least one database to determine whether the addressee has a public key in order to determine the type of encryption to be performed on the package;

~~in response to~~upon a determination that the addressee ~~not having a public key:~~

does have a public key, encrypting the package with the addressee's public key and not encrypting the package with an escrow encryption ~~key;~~

key;

only upon a determination that the addressee does not have a public key, selectively encrypting the package with the escrow encryption key;

storing the escrow key encrypted package in escrow for the addressee prior to receiving a public key for the addressee;

notifying the addressee of the package stored in escrow; and

in response to receiving an acknowledgement from the addressee:

issuing new public and private keys to the addressee, where said new public key is not equal to said escrow encryption key; and

in response to subsequently verified authentication of the addressee:

transmitting the package to the addressee via the network.

2. (Original) The method of claim 1, wherein the step of determining whether the addressee has a public key comprises the sub-step of:

checking a public key directory for a public key of the addressee.

3. (Original) The method of claim 1, further comprising the step of:

storing the addressee's new public key in a public key directory.

4. (Original) The method of claim 1, wherein the encrypting step comprises the sub-steps of:

providing an escrow encryption key and an escrow decryption key,

wherein the escrow encryption and decryption keys comprise one of symmetric keys and asymmetric keys; and

encrypting the package with the escrow encryption key.

5. (Previously Presented) The method of claim 1, wherein the notifying step comprises the sub-step of:

sending a notification to the addressee via the network, wherein said notification includes an attached module for generating private and public keys at the addressee location.

6. (Original) The method of claim 5, wherein the notification comprises one of an e-mail notification, a desktop notification, a voice notification, a pager notification, and a facsimile notification.

7. (Original) The method of claim 1, further comprising the step of:

decrypting the package with an escrow decryption key corresponding to the escrow encryption key.

8. (Original) The method of claim 1, wherein the escrow encryption key is different from the new public and private keys issued to the addressee.

9. (Original) The method of claim 1, wherein the acknowledgement from the addressee includes an indication of the addressee's name and e-mail address.

10. (Original) The method of claim 1, further comprising the step of:

in response to an address having a public key;

encrypting the package with the addressee's public key;

storing the package;

notifying the addressee of the package;

authenticating a user as the addressee by manipulating a message sent by the addressee encrypted using the addressee's private key; and

transmitting the package to the authenticated addressee in response to authenticating the user as the addressee.

11. (Canceled)

12. (Currently Amended) A computer implemented method for securely transmitting an information package to an addressee via a network, the method comprising the steps of:

determining whether to apply escrow encryption to a file by checking at least one electronic directory to determine whether the addressee has a public key; and

only in response to a determination that the addressee has a public key, encrypting the package using the addressee's new public key and transmitting the addressee's new public key encrypted package to the addressee via the network without storing said package in escrow; and

~~not having~~only in response to a determination that the addressee does not have a public key:

encrypting the package with an escrow encryption ~~key;~~key,

storing the escrow key encrypted package in escrow for the addressee;

notifying the addressee of the package in escrow; and

in response to receiving an acknowledgement from the addressee:

issuing new public and private keys to the addressee;

decrypting the package with an escrow decryption key;

re-encrypting the package using the addressee's new public key; and

transmitting the addressee's new public key encrypted package to the addressee via the network, wherein said addressee's new public key is not identical to said escrow encryption key.

13. (Original) The method of claim 12, wherein the step of determining whether the addressee has a public key comprises:

checking a public key directory for a public key of the addressee.

14. (Original) The method of claim 12, further comprising the step of:

storing the addressee's new public key in a public key directory.

15. (Previously Presented) The method of claim 12, wherein the step of transmitting the package comprises the sub-steps of:

authenticating the user as the addressee using a digital signature of addressee; and

transmitting the package to the authenticated user via the network.

16. (Original) The method of claim 12, further comprising the step of:

decrypting the package using he addressee's new private key.

17-27 (Cancelled)

28. (Currently Amended) In a computer-readable medium, a computer program product for securely transmitting an information package to an addressee via a network, the computer-readable medium comprising program code adapted to perform the steps of:

determining whether the addressee has a public key;

only in response to a determination that the addressee ~~not having a public key;~~does have a public key, encrypting the package with the addressee's public key and transmitting the addressee's public key encrypted package to the addressee;

only in response to a determination that the addressee does not have a public key:

encrypting the package with an escrow encryption key;

transmitting the escrow key encrypted file to an escrow storage area and storing the encrypted package in escrow for the addressee;

notifying the addressee of the package in escrow; and

in response to receiving an acknowledgement from the addressee:

transmitting a new public and private keys generation module to the addressee;

issuing new public and private keys at addressee's location, where said new public key is not identical to the escrow encryption key;

contingent upon authentication of the addressee based on a message sent by addressee subsequent in time to the acknowledgement received from the addressee, transmitting the package to the addressee via the network; and

wherein the package is encrypted by at least the escrow key or the addressee's public key during each transmission of the information package across the network until the package is received by the addressee.

29. (Previously Presented) The method of claim 1, wherein said step of authentication of the addressee includes the sub-steps of:

the addressee encrypting a message using addressee' private key;

the addressee sending said private-key encrypted message to the sender;

the sender decrypting said private-key encrypted message using addressee's public key;

the sender authenticating the addressee based on the content of the decryption of said private-key encrypted message.

30. (Previously Presented) The method of claim 1, wherein said step of authentication of the addressee includes the sub-steps of:

the addressee requesting registration with a certificate authority;

the certificate authority registering the addressee subsequent to verifying at least one of the addressee's name, address, telephone number, e-mail address;

the certificate authority generating at least a public key associated with the addressee;

the certificate authority making the public key available for use by the sender; and

the sender authenticating the addressee based on decryption of a message using the public key.

31. (Currently Amended) A computer-implemented method for securely transmitting an information package from a sender to an addressee via a network, the method comprising the steps of:

a sender on a first computer addressing an information package to an addressee;

~~determining~~checking at least one directory to determine whether the addressee has a public key;

only in response to a determination that the addressee has a public key, encrypting the package with the addressee's public key and transmitting the addressee's public key encrypted package to said addressee without waiting for an acknowledgement from the addressee;

~~not having~~only in response to a determination that the addressee does not have a public key:

encrypting the package with an escrow encryption key;

transmitting the escrow key encrypted package through the network to an escrow storage area remote from said first computer;

storing the escrow encrypted package in escrow in said escrow storage area for the addressee prior to receiving a public key for the addressee;

notifying the addressee of the package stored in escrow; and

in response to receiving an acknowledgement from the addressee:

issuing new public and private keys to the addressee; and

in response to subsequently verified authentication of the addressee:

transmitting the encrypted information package to the addressee via the network.

32. (New) A computer-implemented method for securely transmitting an information package from a sender to an addressee via a network, the method comprising the steps of:

a sender on a first computer addressing an information package to an addressee;

checking at least one electronic directory to determine whether the addressee has a public key;

in response to a determination that the addressee has a public key, encrypting the package with the addressee's public key and transmitting the addressee's public key encrypted package to said addressee;

only in response to a determination that the addressee does not have a public key:

encrypting the package with an escrow encryption key and subsequently transmitting the escrow key encrypted package through the network to an escrow storage area on a network computer remote from said first computer;

storing the escrow encrypted package in escrow in said escrow storage area for the addressee prior to receiving a public key for the addressee;

notifying the addressee of the package stored in escrow; and

in response to receiving an acknowledgement from the addressee:

issuing new public and private keys to the addressee; and

in response to subsequently verified authentication of the addressee:

transmitting the encrypted information package to the addressee via the network.

33. (New) The computer-implemented method of claim 32, wherein said escrow encryption key is independent of the computer on which the escrow key encrypted document is stored.

34. (New) The computer-implemented method of claim 32, wherein said escrow encryption key is document dependent.

35. (New) The computer-implemented method of claim 32, wherein said escrow encryption key is addressee public key determination dependent.

36. (New) The computer-implemented method of claim 32, wherein said escrow encryption key is not equal to said addressee's new public key.

37. (New) The computer-implemented method of claim 32, further comprising the step of:

subsequent to the step of issuing the new public encryption key, decrypting the package with an escrow decryption key;

re-encrypting the package using the addressee's new public key prior to the step of transmitting the addressee's new public key encrypted package to the addressee via the network.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☑ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☑ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.